УДК 681.324

В.В. МКРТИЧЯН

О РЕАЛИЗАЦИИ ПРОГРАММНОГО МОДУЛЯ СПИСОЧНОГО ДЕКОДЕРА СУДАНА ДЛЯ КОДОВ РИДА-СОЛОМОНА

Решена задача разработки программного модуля списочного декодера Судана для кодов Рида-Соломона. Получена структурная схема и программная реализация декодера. Особенностью реализации является применение в модуле эффективного алгоритма факторизации Рота-Руккенштейна.
Ключевые слова: *коды Рида-Соломона, списочное декодирование, факторизация многочленов.*

Введение. Одним из мощных методов борьбы с помехами, искажающими информацию в системах ее передачи и хранения, является алгебраическое помехоустойчивое кодирование. Для применения этого метода необходимо выбрать подходящий код и эффективный кодек, работающий на этом коде [1]. В практике цифровой помехоустойчивой связи широкое распространение получили коды Рида-Соломона (РС-коды), при этом перспективным направлением остается разработка для них новых кодеков, способных эффективно работать при большей зашумленности канала. Большим достижением в теории помехоустойчивого кодирования было создание М.Суданом в 1997 году принципиального списочного декодера для РС-кодов [2], который использует интерполяцию и факторизацию многочленов двух переменных над расширением базового поля Галуа и способен с полиномиальной сложностью работать за пределами конструктивного кодового расстояния. Для решения алгоритмически трудной алгебраической задачи факторизации полиномов двух переменных над полем Галуа наилучшим средством в настоящий момент является алгоритм Рота-Руккенштейна [3]. Декодер Судана производит поиск всех кодовых слов, удаленных от пришедшего по каналу слова на расстояние Хемминга, не превышающее значения некоторого управляющего параметра r. Следует отметить, что проблема разработки и технической реализации жестких и мягких списочных декодеров для РС-кодов и более общих алгебро-геометрических кодов актуальна и в настоящее время активно исследуется [4, 5].

Постановка задачи. Цель данной работы – разработка и реализация программного модуля списочного декодера Судана для компьютерной модели цифрового канала передачи данных, использующего в конструкции декодера факторизационный алгоритм Рота-Руккенштейна.

Принципиальный декодер Судана и метод факторизации Рота-Руккенштейна. Пусть $\mathbf{F}_q$ – поле Галуа мощности q с фиксированным примитивным элементом w; $\mathbf{F}_q[x]$ – кольцо полиномов переменной x над полем $\mathbf{F}_q$; $\mathbf{F}_q[x,y]$ – кольцо полиномов двух переменных x и y над полем $\mathbf{F}_q$ [6]. РС-код длины $n=q$ и размерности $k=d+1$ можно определить как множество векторов $\{(p(x_1), p(x_2), p(x_3),\ldots, p(x_n))\}$, где $x_i = w^{i-1}$, $i\in[n]$, а p пробегает множество информационных полиномов, то есть полиномов из $\mathbf{F}_q[x]$ степени не выше d. РС-код достигает границы Синглтона, поэтому кодовое расстояние равно $n\text{-}d$. Взвешенную степень монома x^iy^j определим как $i+dj$, а взвешенную степень $\deg_{(1,d)}(Q)$ полинома Q из $\mathbf{F}_q[x,y]$, определим как наибольшую из взвешенных степеней входящих в него мономов. Далее мощность произвольного множества A будем обозначать через |A|.

Алгоритм Судана включает два основных шага: шаг интерполяции, на котором по принятому из канала слову строится полином двух переменных специального вида, и шаг факторизации, где данный полином разлагается на сомножители, по которым можно построить список. Он имеет полиномиальную оценку сложности $O(n^3)$.

Входными параметрами декодера Судана является некоторый управляющий параметр $t(\in \{0;1;\ldots;n\})$ и параметры РС-кода: длина n, размерность кода k, примитивный элемент w поля F_q. Для корректной работы алгоритма необходимо выполнение ограничения:

$$t \geq d\left\lfloor \sqrt{2(n+1)/d} \right\rfloor - \lfloor d/2 \rfloor$$

(обоснование см. [2]).

При декодировании на вход алгоритма подается пришедшее по каналу слово $y=(y_i)_{i=1}^n$ в виде сетки $\{(x_i, y_i)\}_{i=1}^n$, где $x_i = w^{i-1}$. Декодер Судана производит поиск всех кодовых слов в пределах Хемминговой сферы, центром которой является y, радиусом – величина $r = n - t$. Полученные слова называются связными и образуют искомый список. Величину r будем называть радиусом локации списочного декодера.

Выходом алгоритма является список всех информационных полиномов $f(x)$ $(\in \mathbf{F}_q[x])$, удовлетворяющих условию $|\{i| f(x_i) = y_i\}| \geq t$. Из [2] вытекает, что этот список содержит истинное информационное сообщение.

Алгоритм Судана: /* Вход: $\mathbf{F}_q$, d, t; и сетка $\{(x_1, y_1),\ldots, (x_n, y_n)\}$ */

Шаг 0. Вычислить внутренние параметры m, l :

$m = \lceil d/2 \rceil -1$ и $l = \lceil (2(n+1)/d)^{1/2} \rceil -1$.

Шаг 1. (Интерполяция). Найти любой полином $Q\in \mathbf{F}_q[x,y]$, удовлетворяющий следующим условиям:

1) $\deg_{(1,d)}(Q) \leq m+ld$;

2) $\forall i \in [n]$, $Q(x_i, y_i) = 0$;

3) Q не равен нулю тождественно.

Шаг 2. (Факторизация). Разложить Q на неприводимые сомножители.

Шаг 3. Выдать все полиномы $f(x)$ такие, что $(y - f(x))$ является делителем Q, причем $f(x_i) = y_i$, по крайней мере в t значениях $i\in[n]$

Вычисляемые на нулевом шаге параметры l и m гарантируют существование полинома двух переменных Q, удовлетворяющего всем требованиям первого шага алгоритма Судана, в частности, обнуляющегося во всех точках входной сетки.

Для реализации первого шага алгоритма Судан предложил искать полином Q в виде

$$Q(x,y)=\Sigma_{j=0}^{l}\Sigma_{k=0}^{m+(l-j)d} q_{kj}x^k y^j. \quad (1)$$

Для нахождения коэффициентов q_{kj} рассматривается однородная система линейных уравнений

$$\Sigma_{j=0}^{l}\Sigma_{k=0}^{m+(l-j)d}q_{kj}(x_i)^k(y_i)^j=0,\ i(\in \{0;1;\ldots;n\}), \quad (2)$$

не имеющая в настоящий момент специальных методов решения, то есть решаемая, например, методом Гаусса за время $O(n^3)$. Разрешимость системы обеспечивают значения параметров l,m, рассчитанных на нулевом шаге.

Замечание. Для возможности получения списков разных объемов в ходе декодирования значение управляющего параметра t можно менять с перезапуском последнего шага алгоритма.

Алгоритм Рота-Руккенштейна рассматривает полином двух переменных $Q(x,y)$ ($\in \mathbf{F}_q[x,y]$) [3] как полином переменной y с коэффициентами из $\mathbf{F}_q[x]$: $Q(x,y) = \Sigma_{t=0}^{l} Q^{(t)}(x)\ y^t$ и ищет в кольце $\mathbf{F}_q[x]$ его полиномиальные корни, называемые y-корнями.

В ходе работы алгоритм строит дерево коэффициентов полиномов $f(x)(\in \mathbf{F}_q[x])$, для которых разность $(y - f(x))$ делит полином $Q(x,y)$. Применяя алгоритм Рота-Руккенштейна в списочном декодере Судана, мы получаем все полиномы искомого списка (это вытекает из структуры полинома Q, см. доказательство в [2]), а также другие сомножители вида $(y - f(x))$. Все ненужные сомножители отсеиваются путем проверки связности входящих в них полиномов $f(x)$.

Этот алгоритм реализован в виде рекурсивной процедуры, конструкция и корректность которой основана на следующей теореме.

Теорема. Пусть $f(x)=\Sigma_{s\geq 0} f_s x^s$ – y-корень ненулевого полинома двух переменных $Q(x,y)$ над полем $\mathbf{F}_q$, $h_i(x)=\Sigma_{s\geq i} f_s x^{s-i}$, где $i\geq 0$. Пусть $M_i(x,y)= x^{R_i}$ $Q_i(x, y)$, $Q_{i+1}(x,y)=M_i(x,\ xy+f_i)$, где $Q_0(x,y)=Q(x,y)$, $i\geq 0$, R_i – максимальное целое число, такое что x^{R_i} делит $Q_i(x,\ y)$. Тогда для любого $i\geq 0$ выполняется: $Q_i(x,\ h_i(x)) = 0$, $M_i(0,\ f_i) = 0$.

Входные параметры алгоритма Рота-Руккенштейна: k определяет размерность линейного векторного пространства, в котором осуществляется поиск y-корней полинома Q; i – степень y-корня, при которой на данном шаге алгоритма отыскивается коэффициент; массив S – вектор коэффициентов y-корня. Вызывать процедуру необходимо с параметрами (Q, k, 0).

Алгоритм Рота-Руккенштейна:

procedure Reconstruct ($Q(x,\ y)\neq 0 \in \mathbf{F}_q[x,y]$, $k \in \mathbf{Z}^+$, $i\in \mathbf{Z}$)

/* Глобальный массив S[0,...,k-1] */

Шаг 1. Найти максимальное v ($\in \mathbf{Z}^+\cup\{0\}$), для которого $Q(x,\ y)/x^v$– полином двух переменных.

Шаг 2. $M(x,\ y):= Q(x,\ y)/x^v$.

Шаг 3. Найти все корни γ ($\in \mathbf{F}_q$) полинома одной переменной $M(0,\ y)$.

Шаг 4. Для каждого из γ выполнять{

Шаг 5. S[i] := γ.

Шаг 6. Если $i = k$-1 ,то выдать S[0],...,S[k-1]

иначе {

Шаг 7. $M``(x,\ y) := M(x,\ y + \gamma)$.

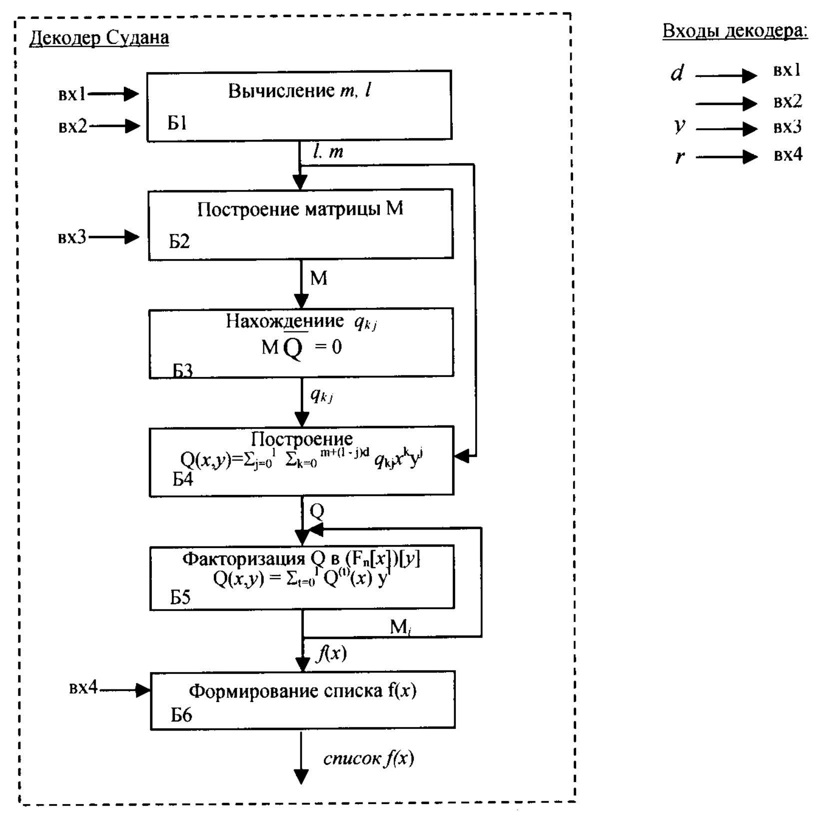
Шаг 8. $M`(x,\ y) := M``(x,\ xy)$.

Шаг 9. Вызвать Reconstruct ($M`(x,\ y)$, k, i+1).

} }

Итак, выходом алгоритма Судана для РС-кодов с алгоритмом Рота-Руккенштейна в качестве второго шага служит список, содержащий в качестве своего элемента истинное сообщение.

Структурная схема списочного декодера. На рисунке, приведенном ниже, изображена схема декодирования, принятого по каналу вектора *y*, и система входов кодека. На вход декодера подаются размерность *k* и длина РС-кода *n*, зашумленный кодовый вектор *y*, радиус локации *r*, помеченные на схеме как ВХ1, ВХ2, ВХ3, ВХ4 соответственно. Декодирование происходит в блоках Б1-Б7. Рассмотрим подробнее работу этих блоков.



Структурная схема списочного декодера, схема входов

Блок Б1 на вход получает *k*, *n* и вычисляет значения параметров декодера *l* и *m*.

Блок Б2 строит матрицу однородной системы (2), обозначенную на схеме буквой М. Построение i-й строки происходит путем вычисления коэффициентов $(x_i)^k(y_i)^j$ при неизвестной q_{kj} ($(x_i, y_i) \in \{(x_i, y_i)\}_{i=1}^{n}$) и присвоения их координатам строки. При этом порядок следования элементов строки несущественен, но в реализации проще использовать естественный порядок, получаемый при раскрытии двойной суммы.

Блок Б3, решая матричную систему $M\overline{Q}=0$ методом Гаусса, где $\overline{Q}$ - вектор-столбец коэффициентов q_{kj} полинома (1), находит коэффициенты q_{kj}.

Блок Б4 по полученным в Б3 коэффициентам q_{kj} строит полином (1).

Блок Б5 представляет реализацию рекурсивной процедуры факторизации полинома (1), основанную на алгоритме Рота-Руккенштейна. Данная процедура в процессе работы строит дерево коэффициентов полиномов, ветви которого образуют список, включающий искомый.

Блок Б6 на вход получает радиус локации кодовых сообщений *r*, который может служить, например, параметром обратной связи в том случае, если декодер является элементом схемы, последующие компоненты которой могут потребовать сокращения объема списка, либо может принимать максимальное значение (см. выше). Б6 кодирует полиномы образованного на предыдущем шаге списка и, выбирая из полученных кодовых слов связные, вычисляет искомый список.

О программной реализации. Рассмотрим некоторые аспекты программной реализации структурной схемы, описанной выше.

Арифметический процессор, служащий основой для вычислений, был реализован на базе динамической библиотеки теоретико-числовых методов WinNTL-5_3_2 (см. например http://shoup.net/ntl/). Данная библиотека позволяет производить вычисления в полях Галуа и содержит реализации алгебраических алгоритмов и структур, необходимых для работы кодека. Например, полиномиальный класс, который удобно использовать для представления истинных информационных полиномов списков в блоке Б6, класс матриц, который удобно использовать при построении матрицы М в блоке Б2, алгоритм Гаусса, используемый в Б3. К сожалению, в данной реализации библиотеки не предусмотрено представление полиномов двух переменных над полями Галуа, однако, наличие такого представления необходимо для реализации списочного декодера Судана. Для получения такой возможности в процессе реализации декодера был написан класс представления полиномов двух переменных на языке С++, использованный в блоках Б4, Б5 для представления полинома Q.

Полином двух переменных $Q\in \mathbf{F}_q[x,y]$ рассматривается как полином одной переменной y с коэффициентами из кольца полиномов $\mathbf{F}_q[x]$, то есть как элемент кольца $(\mathbf{F}_q[x])[y]$. Такое представление позволило реализовать полиномы двух переменных в виде динамического массива указателей на объекты классов полиномов одной переменной. Далее был построен наследник этого класса, включающий реализацию процедуры факторизации полинома двух переменных Рота-Руккенштейна, необходимую для декодера Судана. Благодаря специфике вышеописанного представления возможна эффективная реализация всех вспомогательных процедур класса факторизующегося полинома двух переменных, обращающихся напрямую к полям и методам класса-предка.

Декодер реализован в виде С++ класса, включающего в себя шаг расчета параметров и шаг интерполяции алгоритма Судана. Перенесение шага факторизации в класс представления полиномов двух переменных над полями Галуа значительно снизило функциональную нагрузку на декодер. Эффективность реализации была также повышена путем классификации управляющих параметров декодера на константные и варьируемые. В случае, когда при декодировании изменяются лишь варьируемый параметр *r* - радиус локации, - представляется возможным быстро получить искомый список на основе полученных ранее списков без перестроения структуры декодера.

Структурная схема программно реализована под операционные системы Windows 95/98/NT/2000/XP на основе библиотеки классов MFC [7].

Выводы. Решена задача разработки программного модуля списочного декодера Судана для кодов Рида-Соломона с применением алгоритма факторизации Рота-Руккенештейна. При работе на низкоскоростных кодах данный декодер способен исправлять большее количество ошибок по сравнению с другими декодерами [2, 4], но при этом вместо одного передаваемого сообщения выдает список сообщений, одним из элементов которого является истинное. Поэтому для применения этого декодера в цифровых системах передачи данных помимо разработанного модуля необходим блок, реализующий выделение истинного сообщения из списка. Проблема построения такого блока рассмотрена в работе [8]. Результаты настоящей работы частично представлены в [7].

Библиографический список

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.
2. Sudan M. Decoding of Reed Solomon codes beyond the error correction bound // J. Compl., 13 – 1997. – P. 180-193.
3. Roth R., Ruckenstein G. Efficient decoding of Reed-Solomon codes beyond half of minimum distance // IEEE Transactions on Information Theory. – 2000. – Vol. 45. – P. 432-437.
4. Guruswami V., Sudan M. Improved decoding of Reed-Solomon and algebraic-geometric codes // IEEE Transactions on Information Theory. – 1999. – Vol. 45. – P. 1755-1764.
5. Wu X-W., Siegel P.H. Efficient root finding algorithm with application to list decoding of algebraic-geometric codes // IEEE Transactions on Information Theory. – 2001. – Vol. 47. –P. 2579-2587.
6. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
7. Мкртичян В.В. О программной реализации списочного декодера Судана для кодов Рида-Соломона. // Математические методы в технике и технологиях, ММТТ-18: XVIII международ. науч. конф.: Сб. тр. – Казань. – Т.6. – 2005. – С. 87-88.
8. Маевский А.Э., Мкртичян В.В. Об экспериментальном исследовании списочного декодера Судана для кодов Рида-Соломона // Компьютерные технологии в науке, производстве, социальных и экономических процессах: Мат. V междунар. науч.-практ. конф. ЮРГТУ(НПИ). – Новочеркасск, 2004. – Ч.3. – С. 29-30.

Материал поступил в редакцию 20.03.07.

V.V.MKRTICHAN

ON THE PROGRAM MODULE REALIZATION OF SUDAN DETERMINED DECODER FOR REED-SOLOMON CODES

The program module of Sudan determined list decoder for Reed-Solomon codes is developed. The block diagram and program realization of decoder are constructed. A part of the realization is based on the effective factorization algorithm of Roth-Ruckenstein.

МКРТИЧЯН Вячеслав Виталиевич (р.1982), магистрант кафедры "Программное обеспечение вычислительной техники и автоматизированных систем" ДГТУ. Окончил ДГТУ в 2004 г.
Научные интересы связаны с разработкой математических методов в системах защиты информации.
Автор 7 публикаций.